## CLAIMS

1. A semiconductor integrated circuit for decryption of broadcast signals, comprising:

an input interface for receipt of received encrypted broadcast signals and control data, and an output interface for output of decrypted broadcast signals;

a processing unit arranged to receive encrypted broadcast signals via the input interface, to decrypt the encrypted broadcast signals in accordance with control signals, and to provide decrypted broadcast signals to the output interface;

a first decryption circuit arranged to receive encrypted control signals from the input interface and to decrypt the control signals in accordance with a common key from a common key store;

a second decryption circuit arranged to receive the common key in encrypted form from the input interface and to decrypt the common key in accordance with a secret key from a secret key store;

whereby the circuit is arranged such that the only route to placing a common key in the common key store is to input the common key in encrypted form for decryption in accordance with the secret key, and the only route to providing the control signals to the processing unit is to input them in encrypted form for decryption in accordance with the common key.

2. The semiconductor integrated circuit of claim 1, wherein the first decryption circuit and second decryption circuit are formed in a common circuit.

3. The semiconductor integrated circuit of to claim 1, wherein at least one of the first decryption circuit and the second decryption circuit comprises an AES circuit.

4. The semiconductor integrated circuit of claim 1, wherein the broadcast signal comprises a digital television signal and the processing unit comprises a DVB circuit.

5. The semiconductor integrated circuit of claim 1, wherein the input interface has a separate input for the encrypted common key connected to the decryption circuit.

6. The semiconductor integrated circuit of claim 1, wherein the secret key is unique to the semiconductor integrated circuit.

7. The semiconductor integrated circuit of claim 1, wherein the common key store is arranged to store multiple common keys.

8. A television decoder comprising the semiconductor integrated circuit of claim 1.

9. A system for broadcasting signals to a plurality of subscribers in which only authorized recipients are able to decrypt the broadcast signals, comprising:

a transmitter arranged to broadcast:

signals encrypted according to control words;

control words encrypted according to a common key common to all authorized recipients;

a common key encrypted respectively according to a unique secret key of each authorized recipient; and

a plurality of receivers, each comprising a semiconductor integrated circuit of claim 1, wherein the secret key is unique to each semiconductor integrated circuit.

10. A device for decryption of broadcast signals, comprising:

a common key store configured to receive a common key in encrypted form;

a secret key store configured to store a secret key;

a decryption unit comprising a first decryption circuit configured to receive encrypted control signals and to decrypt the control signals in accordance with the common key from the common key store, and a second decryption circuit configured to receive the common key in encrypted form and to decrypt the common key in accordance with a secret key from the secret key store and to store the common key in the common key store; and

a processing unit configured to receive encrypted broadcast signals and decrypt the encrypted broadcast signals in accordance with the decrypted control signals received from the decryption unit and to provide decrypted broadcast signals to an output interface.

11. The device of claim 10, wherein the common key store is configured to store multiple common keys.

12. The device of claim 10, wherein the decryption device is formed as a single semiconductor integrated circuit having an input interface for receipt of encrypted broadcast signals, encrypted control signals, and encrypted common keys, and an output interface for output of decrypted broadcast signals.

13. A method of decrypting encrypted broadcast signals, comprising:

receiving encrypted broadcast signals, encrypted control signals, and encrypted common key signals at an input interface of a decryption unit formed on a semiconductor integrated circuit;

decrypting the encrypted common key utilizing a stored secret key to generate a common key;

decrypting the encrypted control signals with the common key to generate decrypted control signals; and

decrypting the encrypted broadcast signals in accordance with the control signals and providing decrypted broadcast signals to an output interface of the decryption device.

14. The method of claim 13, further comprising storing a secret key that is unique to the decryption unit in a secret key store in the decryption unit.

15. The method of claim 13, further comprising receiving multiple encrypted common keys, decrypting each of the encrypted common keys to generate multiple decrypted common keys, and storing the multiple decrypted common keys in a common key store in the decryption unit.

16. A method for broadcasting signals to a plurality of subscribers in which only authorized recipients are able to decrypt the broadcast signals, the method comprising:

encrypting control words and transmitting the encrypted control words;

encrypting a common key and transmitting the encrypted common key;

encrypting broadcast signals and transmitting the encrypted broadcast signals to the plurality of subscribers;

providing a secret key to the authorized recipients that is stored in a decryption unit;

receiving encrypted broadcast signals, encrypted control signals, and encrypted common key signals at an input interface of a decryption unit formed on a semiconductor integrated circuit;

decrypting the encrypted common key utilizing a stored secret key to generate a common key;

decrypting the encrypted control signals with the common key to generate decrypted control signals; and

decrypting the encrypted broadcast signals in accordance with the control signals and providing decrypted broadcast signals to an output interface of the decryption device.

17. The method of claim 16, further comprising storing a secret key that is unique to the decryption unit in a secret key store in the decryption unit.

18. The method of claim 16, further comprising receiving multiple encrypted common keys, decrypting each of the encrypted common keys to generate multiple decrypted common keys, and storing the multiple decrypted common keys in a common key store in the decryption unit.

19. A system for broadcasting signals to a plurality of subscribers in which only authorized recipients are able to decrypt the broadcast signals, the system comprising:

a transmitter configured to broadcast signals encrypted according to control words, control words encrypted according to a common key that is common to all authorized recipients, and a common key encrypted according to a secret key that is unique to each authorized recipient; and

a plurality of receivers configured to receive the broadcast signals, each receiver comprising a decryption unit having a secret key unique to the decryption unit stored therein, and each decryption unit further comprising:

a common key store configured to receive a common key in encrypted form;

a secret key store configured to store a secret key;

a decryption unit comprising a first decryption circuit configured to receive encrypted control signals and to decrypt the encrypted control signals in

accordance with a common key from the common key store, and a second decryption circuit configured to receive the common key in encrypted form and to decrypt the encrypted common key in accordance with a secret key from the secret key store and to store the common key in the common key store; and

a processing unit configured to receive encrypted broadcast signals and decrypt the encrypted broadcast signals in accordance with the decrypted control signals received from the decryption unit and to provide decrypted broadcast signals to an output interface.

20. The system of claim 19, wherein the common key store is configured to store multiple common keys.

21. The system of claim 19, wherein the decryption device is formed as a single semiconductor integrated circuit having an input interface for receipt of encrypted broadcast signals, encrypted control signals, and encrypted common keys, and an output interface for output of decrypted broadcast signals.